IN THE SPECIFICATION

Please amend the paragraph beginning on page 3, line 22 as follows:

The processor bus 110 is coupled to a system bus 130 by the chip set ~~125~~ 120. In one embodiment, the system bus 130 is a Peripheral Component Interconnect (PCI) standard bus; however, other bus standards may also be used. Multiple devices, such as an audio device 127, may be coupled to the system bus 130. A bus bridge 140 couples the system bus 130 to a secondary bus 150. In one embodiment, the secondary bus 150 is an Industry Standard Architecture (ISA) bus; however, other bus standards may also be used, for example an Extended Industry Standard Architecture (EISA). A hard drive 153 may be coupled to the secondary bus 150. Other devices, such as cursor control devices (not shown in Figure 1), may be coupled to the secondary bus 150.

A1

Please amend the paragraph beginning on page 9, line 1 as follows:

Any requests to the IDE controller to determine disk characteristics (e.g., number of partitions, type of partition, partition initialization, etc) will not return any valid information about the SPP unless it has been unlocked by submitting a valid master token with the request. Under general circumstances, operating systems and their associated device drivers for hard disks will not pass any sort of token to the IDE controller. Virus software or errant software may pass a token to the IDE controller, but the worst thing that could happen is that such software will keep the IDE controller busy rejecting requests as the rogue software tries all possible number combinations of a potentially large access token (e.g., perhaps ~~40-bit or128-bit~~ 40-bit or 128-bit tokens may used). In one embodiment, the IDE controller may be made intelligent so that after seeing a predetermined number of invalid requests since the last power cycle, the IDE controller disables all access to the SPP or the entire hard drive in recognition of an attempt by the unscrupulous software to gain unauthorized access. In this case, a flag indicating the number of invalid accesses would be reset when the power is turned off. The chances of errant or virus software gaining access to the SPP is limited by the computer system's ability to churn through number permutations but also by a time factor -- it would take a rather long time (e.g., one million years) for a software to run through all possible numbers of a 128-bit token when the power must be cycled off-on after a certain amount of invalid attempts (e.g., 10).

A2